

OBLIVIOUS PROXYING USING A SECURE COPROCESSOR

ABSTRACT OF THE INVENTION

A method, apparatus and system is provided for an entity to facilitate secure communication between a client and server even when they do not support the same set of protocols without violating the trust model which requires that only the client and server be privy to the contents of the communication. In an embodiment this is accomplished by embedding at the site of the proxy an application running inside a secure coprocessor which translates between the protocols that the client supports and those that the server understands. The invention is also useful for purposes such as adaptation of content at the site of the proxy without violating the trust model between the client and the proxy. In general, the scheme describes mechanisms to securely delegate to the infrastructure the ability to enforce an arbitrary trust model between a set of clients and servers participating in some computational task.